USE OF SOCIAL NETWORKING WEBSITES

Directive 3 - 108

Date Issued: July 2013 Amends/Cancels: G.O. 12-09

I. PURPOSE

The purpose of this Directive is to provide guidance to employees of the Department of General Services Maryland Capitol Police (DGS-MCP) on their use of social networking websites. As such, this Directive provides information of a precautionary nature as well as prohibitions on the use of social networking websites.

II. DEFINITIONS

A. **Confidential Information:** Digital photographs, video, audio, or other digital media depicting the Department or its employees, content from criminal or administrative investigations, security procedures, internal videos, daily work activity, or any other information that could be considered sensitive to law enforcement or information that could potentially expose the Department to liability.

B. **Department:** The Maryland Department of General Services (DGS)

C. **Personal Information:** Any type of identifying information including but not limited to ; social security numbers, dates of birth, addresses, phone numbers, e-mail addresses, driver's license or state identification numbers**.**

D. **Post or Posting:** Placing text or digital information publicly on the internet**.**

E. **Social Networking websites**: For the purpose of this policy, social networking websites means computer network sites which focus on building online communities of people who share interests and activities and/or exploring the interest and activities of others. Examples of social networking websites include: Facebook, MySpace, Friendster, Linked In, Twitter, and sites that allow users to post personal blogs. The absence of, or lack of explicit reference to, a specific site does not limit the extent of the application of this Policy as advances in technology will occur and new tools will emerge.

III. BACKGROUND

A. The proper functioning of any law enforcement agency relies upon the public's confidence and trust in the individual officers and the agency to effectively protect and serve the public. Any matter which brings DGS-MCP personnel or DGS itself into disrepute has the corresponding effect of reducing that confidence and trust, as it impedes the ability to work with and serve the public.

B. Professionalism is the most significant factor in providing the highest level of service to the public. While DGS-MCP employees have the right to use personal/social networking web pages or sites when off-duty, as DGS-MCP members, they are public servants who are held to a higher standard than the general public with regard to general and ethical standards. It is the policy of the DGS-MCP to maintain a level of professionalism in both on-duty and off-duty conduct and employees shall not engage in conduct that contradicts or impedes the DGS-MCP mission.

C. The DGS-MCP has a duty to protect the reputation of the organization and its employees, as well as guard against liability and potential legal risk.

III. POLICY

A. Employees are prohibited from accessing social networking websites while on-duty, unless the employee is conducting a criminal or administrative investigation that has been approved by a supervisor.

B. Employees are prohibited from posting messages that criticize or ridicule DGS, DGS-MCP, or any other State agency.

C. Employees should exercise good judgment when networking online. This includes but is not limited to:

1. refraining from speech containing obscene or sexually explicit language, images, or acts and statements or other forms of speech that ridicule, malign, disparage, or otherwise express bias against any race, any religion, or any protected class of individuals; and

2. refraining from posting speech involving themselves or other Department personnel reflecting behavior that would reasonably be considered reckless or irresponsible.

D. Employees shall not represent that they are speaking or acting on behalf of the Department, or that they are representing or presenting the interests of the Department without the express permission of the Chief of Police DGS-MCP.

E. Employees are prohibited from discussing, posting, or in any other way broadcasting or disseminating information on the internet, social networking sites or other mediums of communication, the business of the Department including, but not limited to, the following;

1. Photographs/images, video or audio files, reports, statements or any other documents created or received by the Department, any of its members or that of any allied agency related to any investigation or any other business involving this Department or that of any allied agency.

2. Any other information, to include personal opinion, related to any open investigation involving this Department or that of any allied agency.

F. Employees are prohibited from posting, or disseminating any sexual, violent, racial or ethnically derogatory material, comments, pictures, artwork, video or other references on their websites or through any other means of communication on their websites in such a way as to bring the Department into an unfavorable light.

G. Employees are encouraged to protect their password to prevent unintended or unauthorized use by other persons.

H. Employees are prohibited from posting, transmitting, or disseminating any confidential information or likeness or images of Department logos, emblems, uniforms and other material that specifically identifies the Department or oneself as an employee of the department on any personal electronic communication, social networking websites, web pages and other electronically transmitted material without the permission of the Chief of Police.

IV. GUIDELINES

A. Employees should exercise caution and good judgment when social networking online. Employees should be aware that the content of these social networking sites can be subpoenaed and used in criminal and civil trials to impeach the employee's testimony or to undermine the employee.

B. Employees should realize that any reference to their employment with the DGS-MCP while using social networking environments could compromise their safety and the safety of their family.

C. All electronic communications created, received, or stored on the Department's or State's electronic communications systems are the sole property of the DGS and/or State of Maryland, and not the author, recipient, or user.

D. Employees should be aware that they may be subject to civil litigation or criminal penalties for:

1. Publishing or posting false information that harms the reputation of another person, group, or organization (defamation);

2. Publishing or posting private facts and personal information about someone without their permission that has not been previously revealed to the public, is not of legitimate public concern, and would be offensive to a reasonable person;

3. Using someone else's name, likeness, or other personal attributes without the person's permission for an exploitative purpose; or

4. Publishing the creative work of another, trademarks, or certain confidential business information without the permission of the owner.

E. Employees should expect that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the Department at any time without prior notice.

F. Any employee becoming aware of or having knowledge of a posting or of any website, web page or e-mail in violation of the provision of this Policy shall notify his or her supervisor immediately.